Applicant : Shackleford et al.
Dckt. No. : 100110346-1
Issued : n/a
Serial No. : 09/977,985
Filed : 10/17/2001
Page : 4

a difference of counts of 1s and 0s in said inputs of said truth table generating 0s

for output is less than or equal to a predetermined 0s input difference threshold.

REMARKS

Applicants wish to thank the Examiner for allowing claims 1-16 in the present application. Examiner noted several informalities needing attention, namely, 1) updating co-pending application status 2) correcting grammar in specification and 3) modifying grammar in claim 6 and 12. Applicants have addressed these informalities and in addition identified an additional informality in claim 13. Accordingly, no new matter has been added by these modifications and Applicants believe the case is now in condition for issuance.

Attached hereto is a marked-up version of the changes made to the specification and claims by the current amendment. The attached page is captioned "**Version with markings to show changes made**".

Applicants have made a diligent effort to place the claims in condition for allowance. However, should there remain unresolved issues that require adverse action, it is respectfully requested that the Examiner telephone Leland Wiesner, Applicants' Attorney at (650) 853-1113 so that such issues may be resolved as expeditiously as possible.

Applicant : Shackleford et al.
Dckt. No. : 100110346-1
Issued   : n/a
Serial No. : 09/977,985
Filed   : 10/17/2001
Page   : 5

For these reasons, and in view of the above amendments, this application is now

considered to be in condition for allowance and such action is earnestly solicited.

Respectfully Submitted,

June 27, 2004

Date

Leland Wiesner

Leland Wiesner
Attorney for Applicants
Reg. No. 39424

Leland Wiesner
Attorney
366 Cambridge Ave.
Palo Alto, California 94306
Tel. (650) 853-1113

Applicant : Shackleford et al.
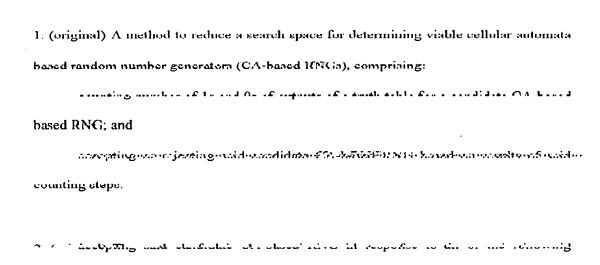Dckt. No. : 100110346-1
Issued   : n/a
Serial No. : 09/977,985
Filed   : 10/17/2001
Page   : 6

Version with markings to show changes made

CLAIMS

What is claimed is:

1. (original) A method to reduce a search space for determining viable cellular automata based random number generators (CA-based RNGs), comprising:

~~counting number of 1s and 0s of outputs of a test table for a candidate CA-based~~ based RNG; and

~~accepting or rejecting said candidate CA-based RNG based on result of said~~ counting steps.

~~2. (currently amended) decrypting said ciphertext at a cluster site in response to the second following~~

Applicant : Shackleford et al.
Dckt. No. : 100110346-1
Issued   : n/a
Serial No. : 09/977,985
Filed   : 10/17/2001
Page   : 7

conditions being met:

a difference of counts of 1s and 0s in said outputs of said truth table is less

than or equal to a predetermined output difference threshold;

a difference of counts of 1s and 0s in said inputs of said truth table

generating 1s for output is less than or equal to a predetermined is input difference

threshold;

and a difference of counts of 1s and 0s in said inputs of said truth table

generating 0s for output is less than or equal to a predetermined 0s input difference

threshold.

3. (original) The method of claim 2, wherein at least one of said predetermined output

difference threshold, predetermined 0s input difference threshold, and predetermined 1s

input difference threshold is zero.

4. (original) The method of claim 1, wherein in said step of accepting or rejecting said

candidate CA-based RNG comprises:

Applicant : Shackleford et al.
Dckt. No. : 100110346-1
Issued   : n/a
Serial No. : 09/977,985
Filed   : 10/17/2001
Page   : 8

 rejecting said candidate CA-based RNG in response to at least one of the following conditions not being met:

 a difference of counts of 1s and 0s in said outputs of said truth table is less than or equal to a predetermined output difference threshold;

 a difference of counts of 1s and 0s in said inputs of said truth table generating 1s for output is less than or equal to a predetermined 1s input difference threshold; and

 a difference of counts of 1s and 0s in said inputs of said truth table generating 0s for output is less than or equal to a predetermined 0s input difference threshold.

5. (original) The method of claim 4, wherein at least one of said predetermined output difference threshold, predetermined 0s input difference threshold, and predetermined 1s input difference threshold is zero.

6. (Currently Amended) A system to reduce a search space for determining viable cellular automata based random number generator (CA-based RNG) [(CA-based RNGs)],

Applicant : Shackleford et al.
Dckt. No. : 100110346-1
Issued   : n/a
Serial No. : 09/977,985
Filed   : 10/17/2001
Page   : 9

comprising:

a truth-table-counting-module counting number of 1s and 0s of outputs of a truth table for a candidate CA-based RNG, said truth-table-counting module also counting number of 1s and 0s of inputs of said truth table for said candidate CA-based RNG; and

a prescreening-module accepting or rejecting said candidate CA-based RNG based on an output or outputs of said truth-table-counting module.

7. (original) The system of claim 6, wherein said truth-table-counting-module comprises:

an output-counting-module counting number of 1s and 0s of said outputs of said truth table for said candidate CA-based RNG; and

an input-counting-module counting number of 1s and 0s of said inputs of said truth table for said candidate CA-based RNG.

8. (original) The system of claim 6, wherein said prescreening-module accepts said candidate CA-based RNG accepts in response to all of the following conditions being met:

Applicant : Shackleford et al.
Dckt. No. : 100110346-1
Issued   : n/a
Serial No. : 09/977,985
Filed   : 10/17/2001
Page   : 10

a difference of counts of 1s and 0s in said outputs of said truth table is less

than or equal to a predetermined output difference threshold;

a difference of counts of 1s and 0s in said inputs of said truth table

generating 1s for output is less than or equal to a predetermined is input difference

threshold; and

a difference of counts of 1s and 0s in said inputs of said truth table

generating 0s for output is less than or equal to a predetermined 0s input difference

threshold.

9. (original) The system of claim 8, wherein at least one of said predetermined output

difference threshold, predetermined 0s input difference threshold, and predetermined is

input difference threshold is zero.

10. (original) The system of claim 6, wherein in said prescreening-module accepts said

candidate CA-based RNG rejects in response to at least one of the following conditions

not being met:

a difference of counts of 1s and 0s in said outputs of said truth table is less

Applicant : Shackleford et al.
Dckt. No. : 100110346-1
Issued   : n/a
Serial No. : 09/977,985
Filed   : 10/17/2001
Page   : 11

than or equal to a predetermined output difference threshold;

a difference of counts of 1s and 0s in said inputs of said truth table generating is for output is less than or equal to a predetermined is input difference threshold; and

a difference of counts of 1s and 0s in said inputs of said truth table generating 0s for output is less than or equal to a predetermined 0s input difference threshold.

11. (original) The system of claim 10, wherein at least one of said predetermined output difference threshold, predetermined 0s input difference threshold, and predetermined 1s input difference threshold is zero.

12. (Currently Amended) A computer readable medium on which is embedded computer software comprising a set of instructions for performing a method to reduce a search space for determining viable cellular automata based random number generator (CA-based RNG) [(CA-based RNGs)], said method comprising:

counting number of 1s and 0s of outputs of a truth table for a candidate CA-based

Applicant : Shackleford et al.
Dckt. No. : 100110346-1
Issued   : n/a
Serial No. : 09/977,985
Filed   : 10/17/2001
Page   : 12

RNG;

counting number of 1s and 0s of inputs of said truth table for said candidate CA-based RNG; and

accepting or rejecting said candidate CA-based RNG based on results of said counting steps.

13.(Currently Amended) The computer readable medium of claim 12, wherein in said method [[(200)]], said step of accepting or rejecting said candidate CA-based RNG comprises:

accepting said candidate CA-based RNG in response to all of the following conditions being met:

a difference of counts of 1s and 0s in said outputs of said truth table is less than or equal to a predetermined output difference threshold;

a difference of counts of 1s and 0s in said inputs of said truth table generating is for output is less than or equal to a predetermined is input difference threshold; and

a difference of counts of 1s and 0s in said inputs of said truth table

Applicant : Shackleford et al.
Dckt. No. : 100110346-1
Issued : n/a
Serial No. : 09/977,985
Filed : 10/17/2001
Page : 13

generating 0s for output is less than or equal to a predetermined 0s input difference

threshold.

14. (original) The computer readable medium of claim 13, wherein at least one of said

predetermined output difference threshold, predetermined 0s input difference threshold,

and predetermined is input difference threshold is zero.

15. (original) The computer readable medium of claim 12, wherein in said method, said

step of accepting or rejecting said candidate CA-based RNG comprises:

rejecting said candidate CA-based RNG in response to at least one of the

following conditions not being met:

a difference of counts of 1s and 0s in said outputs of said truth table is less

than or equal to a predetermined output difference threshold;

a difference of counts of 1s and 0s in said inputs of said truth table

generating 1s for output is less than or equal to a predetermined is input difference

threshold; and

a difference of counts of 1s and 0s in said inputs of said truth table

Applicant : Shackleford et al.
Dckt. No. : 100110346-1
Issued   : n/a
Serial No. : 09/977,985
Filed   : 10/17/2001
Page   : 14

generating 0s for output is less than or equal to a predetermined 0s input difference

threshold.

16. (original) The computer readable medium of claim 15, wherein at least one of said

predetermined output difference threshold, predetermined 0s input difference threshold,

and predetermined is input difference threshold is zero.